IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA	)	**DOCKET NO. 3:22-cr-00157-KDB**
	)	
v.	)	
	)	
DAVID TATUM	)	
	)	

UNITED STATES OF AMERICA'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE AND REQUEST FOR EVIDENTIARY HEARING

The United States of America submits this response in opposition to Defendant's "Motion to Suppress Evidence and Request for Evidentiary Hearing." Defendant's motion fails to raise any cognizable claim for suppression. The only relief he articulates is for a *Franks* hearing, and he has failed to meet his burden for that relief as well. Accordingly, his motion should be summarily denied. Alternatively, his motion should be denied on the merits.

At the Status Conference, Defendant represented to this Court that he would file a motion to suppress. He explained that the motion was based on an illegal search performed by a private actor, Defendant's sister-in-law Courtney Martin. On April 24, 2023, Defendant filed his pleading, titled "Motion to Suppress Evidence and Request for Evidentiary Hearing." The motion, however, fails to sufficiently articulate any legal theory in support of suppression. The motion articulates facts that would support the private actor theory Defendant articulated at the Status Conference but provides only boilerplate Fourth Amendment language under the heading, "Extrajudicial Searches and Illegal Gathering of Evidence." Yet, the motion inexplicably does not explain the basis for suppression. Instead, the motion requests a *Franks* hearing as an impermissible fishing expedition to purportedly "aid in the determination [of] **additional** suppression matters relevant to not only the probable cause underlying the search warrants in this case, but also with respect to

other evidence that may be called into question in light of recent disclosures about the origins of this investigation." (Emphasis added). Read in the light most favorable to Defendant, he wants to buy more time and an opportunity to further develop a Fourth Amendment claim. That is dissonant with respect to the representations Defendant made in the Status Conference and the trial date.

The Defendant's approach puts the Government in the position of not knowing what to respond to. On the one hand, a generous reading of the Defendant's motion, combined with his argument at the Status Conference, arguably suffices to frame the motion to suppress that defense counsel articulated, as well as to address his request for a *Franks* hearing. On the other hand, the motion, by itself, utterly fails to raise, develop, and articulate a cognizable suppression issue and instead impermissibly seeks an evidentiary hearing for the express purpose of obtaining "additional evidence not yet revealed." Faced with this Hobson's choice and a trial slated to start May 2, 2023, with out-of-town civilian witnesses, including the victim who is the subject of Counts 2 and 3, the government will respond to all of Defendant's collective allegations.

Defendant's "Motion to Suppress" and incorporated request for a *Franks* hearing should be denied for the following reasons:

1. Defendant had **no expectation of privacy** in unsecured files he stored on a computer that he jointly shared with his wife.

2. Even if Defendant had an expectation of privacy, Defendant's wife and her sister were **private actors** who conducted the search without the government's knowledge or acquiescence and for the wife's own purpose.

3. Defendant has failed to meet his burden to trigger a *Franks* hearing, but even if he did, there is **no *Franks* violation** because the (i) affiant did not intend to mislead the magistrate judge or omit any relevant information and (ii) the alleged omissions are immaterial

4. Even if Defendant's wife and/or her sister were acting as an instrument or agent of the government or a *Franks* violation occurred, the **remedy** would be to excise the tainted probable cause from the FBI's warrant for Defendant's electronic devices, and

the remaining, untainted probable cause based on Defendant's admissions during his interview with the FBI is sufficient to establish probable cause for the warrant.

5. Even if excising the tainted probable cause results in a warrant without probable cause, the FBI special agents acted in **good faith** reliance on the warrant.

I. Background

In the early morning hours of August 14, 2021, Defendant's wife, Kimberly Tatum ("Kimberly"), went to their shared home office to look at the MacBook that Defendant and Kimberly shared. Kimberly saw nude images of minors. She did not know whether the content of what she saw was illegal, but she nevertheless decided that it was time to divorce Defendant. She was scared that Defendant would retaliate and hurt her or their minor daughter. Accordingly, she recorded what she saw on the MacBook with her phone so that she would have the evidence she needed to support her allegations in civil divorce and custody proceedings. Kimberly later told her sister, Courtney Martin ("Courtney"), and her father, Michael Martin ("Michael"), that she had seen nude images of young girls on their shared computer and wanted to divorce Defendant. Kimberly emailed some of the images she had recorded to Michael. She also attempted to install spyware on the MacBook so that she could learn the extent of Defendant's computer activities.

Upon deciding that she needed to divorce Defendant, Kimberly took steps to reactivate her nursing license so that she could reenter the workforce and hire a divorce attorney. In an effort to protect her daughter from Defendant, Kimberly downloaded the pictures on her phone to a USB drive ("USB A") and gave it to Courtney with the instruction that if anything should happen to her, Courtney should use USB A to protect her daughter.

Sometime in early-to-mid- September, Michael met with Courtney and made two copies ("USB B" and "USB C") of USB A. Michael added the emails that Kimberly had sent him to USB B and USB C. Courtney reorganized the files in USB B and USB C so that USB B could be given

to Kimberly's divorce attorney and USB C would remain with Courtney as an "insurance policy" in case Defendant harmed Kimberly or her daughter. Kimberly retained USB A.

Kimberly met with her divorce attorney around September 20 and provided him USB B. The divorce attorney consulted with a criminal defense attorney, who saw the images on USB B and said that this matter should be reported to the authorities for further investigation. Kimberly told Courtney, and Courtney called the FBI Charlotte Crimes Against Children Supervisor, Kevin Swanson, to report the information. Accordingly, Serial 1 in this investigation begins, "An FBI employee referred the following information on 9/21/2021." (ECF No. 41.4.)

It is no family secret that Courtney worked for the FBI. She has held several administrative positions with the FBI since 2010. In August 2021, Courtney was a Resident Agency Specialist ("RAS") in the Fayettville Office for the FBI. An RAS is an administrative position. The duties include answering the door, escorting visitors, and coordinating office moves. Courtney has no investigative role in any criminal case and has never received training on criminal investigations. Courtney never instructed Kimberly to make any recordings of Defendant's computer activities and, in fact, was more concerned for Kimberly's safety because of the recordings. She believed that if Defendant found out that Kimberly recorded Defendant's computer activities, he would hurt Kimberly. Additionally, Courtney never instructed Kimberly to install any spyware to monitor Defendant's computer activities.

Michael retired in 2005 from being a criminal special agent with various federal agencies, none of which were the FBI. He never investigated child exploitation matters, and he never instructed Kimberly to make any recordings of Defendant's computer activities.

On the morning of September 22, 2021, the FBI case agents in this matter met with Kimberly and her attorney. They discussed what Kimberly had seen and received USB B, two hard

drives, and several phones.[1] They went back to the FBI, reviewed the contents of USB B, and confirmed that the videos that Kimberly recorded depicted child pornography. Based on this information, later that afternoon/evening, the agents went to the medical facility where Defendant worked.

Defendant agreed to speak with the FBI agents in the parking lot of the medical facility. Defendant's admissions were summarized in the affidavit in support of the search warrant for Defendant's devices:

> TATUM had a MacBook laptop computer which he used to manage patient records, of which 75 percent are children. TATUM had a user profile on the laptop which was password protected. KIMBERLY also used the same user profile and accessed the profile using the same password. TATUM obtained images of teen girls from a website called "teen gallery." When TATUM saw a girl whom he thought was attractive, TATUM would input the image in a "deep fake" website which would make the girl in the image appear nude. TATUM advised he first used deep fake websites about four to five years ago. TATUM was asked if the girls he input in the deep fake website were over the age of 18, to which TATUM responded, "it's it's possible but questionable. I'm sorry." When asked if any reasonable person would think the images in question were of a persons under the age of 18 or under the age of 13, TATUM responded, "I don't think any reasonable person would think they are under the age of 13. I think it's possible people might think under the age of 18 is possible. But I didn't go and go and like I don't know what their ages are." TATUM admitted he masturbated to a photograph of an ex-girlfriend, when she was a minor, which TATUM input on the deep fake website resulting in a nude image of the ex-girlfriend. TATUM further admitted to saving these images to zip drives or thumb drives which were unencrypted and stored at his office at home. When asked about external storage devices, TATUM advised he stored pornography on drives.

[1] A forensic analysis later revealed that one of the hard drives, the My Passport, was password protected and encrypted. It contained a video of child pornography involving two completely naked minor girls, approximately 11-13 years old, engaging in continuous sexual activity with each other for approximately 9 minutes (Count 1). It also contained Defendant's production, or attempted production, of child pornography involving his 15 year-old cousin (Counts 1, 2, and 3). One of the phones contains forensic information that it was the phone that Defendant used to make the surreptitious recording of his cousin. Both devices contain attribution evidence establishing Defendant as the user.

Id. at ¶ 20. Agents also seized a MacBook and a USB from a bag Defendant had with him.[2]

While the case agents interviewed Defendant, a separate team of agents went to Defendant's home. Kimberly was there and consented to a search of the common areas. One common area was the office where Kimberly had taken the recordings of the MacBook screen. In that office, agents found an HP computer.[3]

The following day, on September 23, 2021, Courtney's supervisor collected USB C from Courtney. While the Defendant complains that he never knew that Courtney was the "FBI employee" who reported this case to the FBI (ECF No. 41.4), the report collecting USB C from Courtney explicitly identified Courtney by name (ECF No. 41.7). The first time that agents ever interviewed Courtney was on April 14, 2023.[4]

On September 30, 2021, the FBI submitted an application to search the electronic devices at issue in this case. (ECF No. 41.1, 41.2.) As with all warrants, the affiant made clear that "[t]his Affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter." (ECF No. 41.1 at ¶ 3.)

---

[2] The USB contains Defendant's collection of child pornography involving morphed images of minors (Count 1). The MacBook contains a list of 1,118 file names consistent with child pornography, all of which included the phrase "PTHC" (pre-teen hard core), and another list of videos that were played with names that are consistent with child pornography (Count 1). The MacBook further contains evidence that the video of the 15 year old cousin and the morphed images were displayed using the MacBook. User attribution establishes Defendant as the user for both of these devices.

[3] The HP computer contains two videos that depict child pornography (Count 1). User attribution establishes Defendant as the user.

[4] The United States has no intention of presenting at trial the testimony of Courtney Martin. The interview was conducted after a meeting with defense counsel on April 10, 2023 where he raised questions concerning Courtney's involvement in the investigation. The United States has not received any discovery from the Defendant so is unaware of any attempts by Defendant to interview Courtney Martin.

II. Analysis

Defendant's collective arguments from the Status Conference and his "Motion to Suppress" raise two issues: (a) the Private Search Doctrine and (b) a *Franks* hearing. Both issues are discussed below, followed by (c) probable cause for the warrant and (d) the good faith exception. But the Court need not even reach these arguments because it is undisputed that Defendant and Kimberly both had access to the MacBook. See Motion to Suppress at 1 ("In August of 2021, Kimberly Tatum (the Defendant's wife) reportedly observed several concerning images in a folder on the desktop of a MacBook laptop computer, which the couple jointly uses."). As developed below, this fact is dispositive because it demonstrates that Defendant had no expectation of privacy in that computer and therefore is incapable of making a cognizable Fourth Amendment claim.

a. The Private Search Doctrine

Less than two years ago, this Court summarized some of the relevant law on searches by private actors in an order denying a motion to suppress that was filed by the same defense attorney who represents Defendant in this matter. *See United States v. Bonds*, No. 521CR00043KDBDCK, 2021 WL 4782270 (W.D.N.C. Oct. 13, 2021). As a starting point, this Court explained:

> The Fourth Amendment of the United States Constitution guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures… and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. It is well-settled that Fourth Amendment protection extends to a person's electronically stored files, data, e-mail attachments, and the like. *See Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)). Fundamental to the Fourth amendment is that it protects the rights of the people against conduct by the government, not private individuals. *See United States v. Richardson*, 607 F.3d 357, 364 (4th Cir. 2010).

Id. at *2. The case law regarding searches conducted by private actors stems from this concept.

1. Expectation of Privacy From Searches Conducted By Private Actors

With regard to the Private Search Doctrine, this Court in *Bonds* explained that there is no expectation of privacy when information is revealed to a third party. *Id.* at 3. The Court explained:

> The "private search" doctrine is implicated when a private party conducts a search of private information and the government subsequently reviews that same information without first obtaining a search warrant. *United States v. Fall*, 955 F.3d 363, 370 (4th Cir. 2020). The "private search" doctrine's foundation is built on the rule that one can only invoke the Fourth Amendment's protection where he has a legitimate expectation of privacy. *Rakas v. Illinois*, 439 U.S. 128, 143 (1978); *see also Oliver v. United States*, 466 U.S. 170, 177 (1984) (A legitimate expectation of privacy is both subjective and objective in nature. A defendant must show that he had a subjective expectation of privacy; and the expectation is one that society recognizes as reasonable). However, once invoked, an individual's expectation of privacy does not last indefinitely. An expectation of privacy can be "frustrated", or in other words, it can be eliminated. In this circumstance, the Fourth Amendment no longer offers protection from governmental intrusion. The most common example of when an expectation of privacy is frustrated is when information is revealed to a third party. *United States v. Jacobsen*, 466 U.S. 109, 117 (1984) ("[i]t is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information."). The "private search" doctrine consequently allows the government to search where an individual's expectation of privacy has already been frustrated by an initial private search without implicating the Fourth Amendment.
>
> The Supreme Court's decision in *United States v. Jacobsen* best articulates the "private search" doctrine in practice. In *Jacobsen*, FedEx employees found what they believed to be illegal drugs in a damaged box after they had opened it. *Id.* at 111. The United States Drug Enforcement Administration ("DEA") was notified by FedEx and the drugs were placed back in the box until their arrival. *Id.* When the DEA arrived, they replicated the search previously performed by the FedEx employees. *Id.* at 111-112. The Supreme Court held that the Fourth Amendment is not implicated when a private entity acts in a private capacity and that a private search frustrates an expectation of privacy. *Id.* at 117. Thus, law enforcement does not violate the Fourth Amendment when they simply replicate the initial private search. *Id.* ("[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated); *United States v. Fall*, 955 F.3d at 370; *United States v. Runyan*, 275 F.3d 449, 461 (5th Cir. 2001) (Under the private search doctrine, "the critical inquiry under the Fourth Amendment is whether the authorities obtained information with respect to which the defendant's expectation of privacy has not

> already been frustrated"); *see also Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971) (The police need not "avert their eyes" when presented with evidence obtained in a private search).
>
> In *Jacobsen*, the Fourth Amendment was not implicated because the DEA's search of the box allowed the agents to learn "nothing that had not previously been learned during the private search." *Id.* at 120. This established that under the "private search" doctrine invasions of privacy by the government must be tested by the degree they exceed or expand the initial private search. *Id.* at 115; *see also United States v. Fall*, 955 F.3d at 370. Therefore, to determine whether the "private search" doctrine is appropriate in this case, the controlling question the Court must answer is whether Det. Lawing exceeded the private search conducted by Google. If he did, then the Defendant's rights under the Fourth Amendment were violated.

Bonds, 2021 WL 4782270, at 2-3.

Circuits applying this framework to cases involving spouses who have caught their husbands with child pornography have approved a search of the devices as long as law enforcement only saw what the wife previously saw. *See, e.g. United States v. Rivera-Morales*, 961 F.3d 1, 11 (1st Cir. 2020) (upholding officers' review of a video on Defendant's cellphone, which wife had seized and played for officers, and where the video depicted Defendant engaged in sexual activity with daughter); *Rann v. Atchison*, 689 F.3d 832, 834 (7th Cir. 2012) ("Because [the victim] and her mother knew the contents of the digital media devices when they delivered them to the police, the police were 'substantially certain' the devices contained child pornography."); *United States v. Starr*, 533 F.3d 985, 995 (8th Cir. 2008) (upholding search of photo albums, photo prints, and videotapes seized by defendant's wife where wife told police that she was leaving her husband and wanted to report his suspected illegal conduct and police only viewed material that had already been viewed by wife); *United States v. Runyan*, 275 F.3d 449, 464 (5th Cir.2001) (holding that where the defendant's ex-wife had previously viewed files on a disk and confirmed they contained child pornography, the police's after-occurring inspection was permissible).

In this case, there is no dispute that Defendant and Kimberly both had access to the MacBook. *See* Motion to Suppress at 1 ("In August of 2021, Kimberly Tatum (the Defendant's wife) reportedly observed several concerning images in a folder on the desktop of a MacBook laptop computer, which the couple jointly uses."). Moreover, the FBI was virtually, and quite literally, certain that they were only viewing the same images that Kimberly had seen because they only reviewed Kimberly's video recording of the MacBook. In other words, there was no risk here that the FBI could see something beyond what Kimberly saw.

Accordingly, the answer to the "controlling question" is a resounding, "NO," the FBI did not exceed the private search conducted by Kimberly. As a result, Defendant had no expectation of privacy in the images on his computer that Kimberly showed the FBI.[5]

2. Application of the Fourth Amendment to Searches Conducted By Private Actors

Although the Fourth Amendment protects the rights of the people against conduct by the government, it still applies to searches conducted by private actors "if that individual is 'acting as

[5] A related concept here is whether Kimberly could have given consent to search the MacBook. The Fourth Circuit has upheld the denial of a motion to suppress the fruits of an unlawful search of password protected files where law enforcement "reasonably believed" that the defendant's ex-wife had authority to consent to a search of defendant's computer. *See United States v. Buckner*, 473 F.3d 551, 555 (4th Cir. 2007) ("The Government need not establish that Michelle Buckner had actual authority to consent to a search of Buckner's password-protected files in order to succeed on appeal. Rather, it would be sufficient that Michelle had apparent authority to consent to the search at issue."). In *Buckner*, the ex-wife gave law enforcement consent to "take whatever [they] needed" from the home and "whatever [they] found that [they] thought was important to the investigation." *Id.* The Court held that this "unquestionably provided the officers with valid consent to seize and search any items in the home over which Michelle had common authority," which included Defendant's computer. *Id.* The computer was on and the screen was lit despite the fact that the defendant was not present, the ex-wife had leased the computer and had the ability to return it to the rental agency, and there was no indication that any files were password-protected. *Id.* Similarly, Kimberly had access to the MacBook, she told FBI that she shared it with Defendant, Defendant admitted during his interview that Kimberly used the same user profile and accessed the profile using the same password, and none of the child pornography files she saw were further protected by a password. Accordingly, she could have authorized consent to search the MacBook.

an agent of the Government or with the participation or knowledge of any governmental official.'" *United States v. Ellyson*, 326 F.3d 522, 527–28 (4th Cir. 2003) (citing *Jacobsen*, 466 U.S. at 113); *see also Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971) (explaining that a private search may be converted into state action only if the private actor is "regarded as having acted as an 'instrument' or agent of the state"). "The burden of proving that a private party acted as an agent or instrument of the government is on the defendant." *Ellyson*, 326 F.3d at 527 (citing *United States v. Shahid*, 117 F.3d 322, 325 (7th Cir. 1997)). "Whether an agency relationship exists is a fact-intensive inquiry that is guided by common law agency principles." *Id.* (citing *United States v. Koenig*, 856 F.2d 843, 847 n. 1 (7th Cir. 1988)).

In determining whether an agency relationship existed, the Court must determine (A) "whether the government knew of and acquiesced in the intrusive conduct" and (B) "whether the private party's purpose for conducting the search was to assist law enforcement efforts or to further her own ends." *Ellyson*, 326 F.3d at 527 (citations omitted); *United States v. Kinney*, 953 F.2d 863, 865 (4th Cir.1992) (affirming the district court's conclusion that no agency relationship existed where the private individual "acted on her own initiative, without suggestion from the police officers"). Regarding the first factor, "simple acquiescence by the Government does not suffice to transform a private search into a Government search. Rather, there must be some evidence of Government participation in or affirmative encouragement of the private search before a court will hold it unconstitutional. Passive acceptance by the Government is not enough." *United States v. Jarrett*, 338 F.3d 339, 345–46 (4th Cir. 2003).

i. The FBI Did Not Know of or Acquiesce in Kimberly's Search

The FBI had no knowledge of Kimberly's search. In fact, once they learned about this case on September 21, 2021, a case was opened and agents interviewed Kimberly the following

morning. (ECF No. 41.4.) At the Status Conference, however, defense counsel suggested that somehow Courtney was "the government" and that she acquiesced in the search. The facts do not support a finding that Courtney was "the government." Although Courtney was employed by the FBI, she held an administrative role. She was not a criminal investigator and never received training on criminal investigations. Additionally, she did not learn about Kimberly's searches until after Kimberly made them. This hardly constitutes "evidence of Government participation in or affirmative encouragement." *Jarrett*, 338 F.3d at 346.

Even if Courtney were a criminal investigator and she knew or acquiesced in the search, she was acting in her capacity as Kimberly's sister. Without more, the fact that someone works for law enforcement does not convert all of their conduct into government-sponsored conduct. For example, in *United States v. McGreevy*, 652 F.2d 849 (9th Cir.1981), the Ninth Circuit concluded that an off-duty police officer who was working for Federal Express was not acting as an instrument of the state when he opened a package and found contraband. *McGreevy*, 652 F.2d at 851. The Ninth Circuit commented that, "[the off-duty police officer] did not hold his Federal Express position because he was a police officer. He carefully separated the two jobs. He knew of no understanding between Federal Express and the DEA for the disposal of contraband." *Id.* Contrast this case with *State v. Carter*, 267 N.W.2d 385, 386 (Iowa 1978), where the court held that off-duty police officers who conducted a search were not private individuals because "[t]he men were police officers, they were in uniform, they carried sidearms. The record shows arrests were made by these guards as Des Moines police officers. Most significant of all, the whole arrangement was effected in cooperation with the Des Moines Police Department." *Carter*, 267 N.W.2d at 386. Here, the only time that Courtney turned to her position with the FBI was to report

it. Accordingly, Defendant cannot establish that the FBI knew of or acquiesced in Kimberly's search.

ii. Kimberly Searched the MacBook for Her Own Purposes

Kimberly recorded the images on the MacBook for her own purposes. She decided that she was getting divorced and began collecting evidence to divorce him and protect their daughter against him. This is corroborated by the undisputed fact that Kimberly reported her recordings to her civil divorce attorney before she ever reported it to law enforcement. Accordingly, Defendant cannot establish that Kimberly's purpose in conducting the search was to assist law enforcement in prosecuting Defendant.

b. *Franks* Hearing

Defendant has not made the "substantial preliminary showing" under *Franks v. Delaware*, 438 U.S. 154 (1978), that is required for him to obtain an evidentiary hearing challenging the integrity of the affidavit submitted in support of the search warrant in this matter. Moreover, the search warrant affidavit provided ample probable cause to search the devices at issue, which ultimately identified child pornography files.

i. Legal Standard

A *Franks* hearing allows a defendant, in "limited" circumstances, to challenge a search-warrant affidavit. *United States v. Moody*, 931 F.3d 366, 370 (4th Cir. 2019); *United States v. Tate*, 524 F.3d 449, 454 (4th Cir. 2008). The defendant's burden is high. To trigger a *Franks* hearing when the allegation is that the affidavit contains false statements, the defendant must make a "substantial preliminary showing" that the affiant made (1) a false statement, (2) "knowingly and intentionally, or with reckless disregard for the truth," that was (3) "necessary to the finding of probable cause." *United States v. White*, 850 F.3d 667, 673 (4th Cir. 2017) (citing *Franks v. Delaware*, 438 U.S.

154, 155 56 (1978)); *United States v. Moody*, 931 F.3d 366, 370 (4th Cir. 2019). A "presumption of validity" attaches to the affidavit under this analysis. *Tate*, 524 F.3d at 454 (citation omitted). To overcome that presumption, the defendant must offer proof. *Id*. (citation omitted). It is not enough to "point out specifically the portion of the affidavit that is claimed to be false and give reasons why it is false." *Id*. (citation omitted). Rather, the defendant must "furnish affidavits or sworn or otherwise reliable statements of witnesses or explain their absence." *Id*. (citation and alterations omitted). Nor is it sufficient to show "negligence or innocent mistake[s]." *Id.* With all these requirements, the "burden of making the necessary showing is thus a heavy one to bear." *Id*.

To obtain a *Franks* hearing based on an omission theory, a defendant is "required to make a 'substantial preliminary showing' that the omissions were intentional or reckless, and that the omitted information was material to the magistrate's probable cause determination." *United States v. Jones*, 942 F.3d 634, 640 (4th Cir. 2017) (citations omitted). "For the omitted statements to be deemed material, their inclusion must defeat probable cause." *Id*. Accordingly, when a defendant bases his *Franks* request on an omission, as Defendant does here, the "burden increases yet more." *Id.* "An affiant cannot be expected to include in an affidavit every piece of information gathered in the course of an investigation." *United States v. Colkley*, 899 F.2d 297, 300 (4th Cir. 1990) *Id*. Thus, to satisfy *Franks* based on an omission, "the defendant must show that facts were omitted with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading." *Tate*, 524 F.3d at 455 (citation and internal quotation marks omitted). The omissions, if included in the affidavit, "must be essential to the probable cause determination." *Colkley*, 899 F.2d at 300 (citation omitted).

Defendant has fallen considerably short of meeting this high burden. Defendant cannot point to any credible or competent evidence in support of his claim that the affiant omitted the

claimed facts with the intent to mislead the magistrate or in reckless disregard for the truth. Similarly, with respect to the alleged false statement, Defendant points to no evidence that the affiant "knowingly and intentionally, or with reckless disregard for the truth" made an affirmative false statement.

ii. Defendant Has Failed to Offer Evidence that Affiant Intended to Mislead the Magistrate Judge or Omitted Information With Reckless Disregard of Whether it Would Make the Affidavit Misleading

The initial premise of Defendant's claimed omission is based on incorrect facts. Defendant alleges that affiant omitted information disclosing Courtney as an FBI employee who was "extensively involved in the origins of this case." (ECF No. 41 at 11.) He further claims that "Courtney involved herself in conducting an extrajudicial investigation by advising and directly assisting in the collection of evidence over the course of five or six weeks and several trips to Charlotte." *Id.* at 13. He goes on to allege that certain information that was reported in an interview of Courtney, conducted on April 15, 2023 (ECF No. 41.3), was known to the affiant on September 30, 2021, when he submitted the affidavit (ECF No. 41 at 14.). None of this is factually accurate.

Even if accurate, with respect to a *Franks* claim based on alleged omissions, Defendant must show that "the omission is the product of a 'deliberate falsehood or of reckless disregard for the truth.'" *Colkley,* 899 F.2d at 301. Put another way, Defendant is required to offer proof that the affiant "had the requisite intent to mislead." *Id.* at 301. This rule makes good sense because to permit otherwise "potentially opens officers to endless conjecture about investigative leads, fragments of information, or other matter that might, if included, have redounded to defendant's benefit." *Id*. at 301. "Merely identifying [false statements or] factual omissions is insufficient." *United States v. Clenney*, 631 F.3d 658, 664 (4th Cir. 2011). Indeed, *Franks* contemplates that affiants will sometimes get things wrong: "This does not mean 'truthful' in the sense that every

fact recited in the warrant affidavit is necessarily correct, for probable cause may be founded upon hearsay and upon information received from informants." 438 U.S. at 165. As the *Franks* Court acknowledges, the information "sometimes must be garnered hastily." *Id*. Rather, *Franks* examines whether the information "is believed or appropriately accepted by the affiant as true." *Id.* Indeed, as noted by the Fourth Circuit: "*Franks*, by contrast, recognizes that the information an affiant reports from an informant may not ultimately be accurate, and is willing to tolerate such a result so long as the affiant did not mislead the magistrate." *Colkley*, 899 F.2d at 303 (citation omitted).

Here, Defendant has offered no evidence of an intent to mislead the Magistrate Judge. Defendant's motion does not include any supporting attachments containing affidavits or any other supporting evidence. Instead, Defendant invents facts based on speculation and mischaracterization of reports. (*See, e.g.*, "Courtney involved herself in conducting an extrajudicial investigation by advising and directly assisting in the collection of evidence over the course of five or six weeks and several trips to Charlotte." Defendant Motion at 13).

Accordingly, the Court should deny Defendant's request for a *Franks* hearing.

iii. The Alleged Omissions are Immaterial and Do Not Trigger a *Franks* Hearing

To satisfy the *Franks* materiality requirement, the Fourth Circuit has outlined a straight-forward test:

> We assess materiality using a simple test. We insert the omitted facts into the warrant affidavit and, examining the information contained within the "revised" affidavit, evaluate whether there nevertheless would have been probable cause to issue the warrant. If the revised affidavit still establishes probable cause, the defendant is not entitled to a *Franks* hearing

United States v. Jones, 942 F.3d 634, 640 (4th Cir. 2017) (citation omitted).

Here, it is difficult to understand what the omitted facts are that Defendant claims should have been disclosed because he does not articulate them with precision. This is further complicated by the fact that the parties disagree on Defendant's recitation of the facts.

Even taking Defendant's misstated facts as true, these facts are immaterial to probable cause. At the end of his motion, Defendant asks a series of questions that purport to highlight to materiality of the alleged omissions:

> Would it not have been beneficial for the Court to know, prior to signing a warrant, that the flash drive noted in the Affidavit and insinuated to be the original copy created by Kimberly Tatum, was not in fact original nor created by her? And was in fact created by an active FBI employee? And that the original is no longer available because the Government's primary witness at the time smashed it to pieces with a hammer?

ECF No. 41 at 15.

None of these issues impact probable cause in support of the warrant. The affiant reviewed a recording of a MacBook that depicted images of child pornography. The affiant asked Defendant about those images, and he admitted that he made them, he used a deepfake website to make them, and that he masturbated to at least one of them. He further admitted to using the MacBook to make them and to storing those images on various devices, including USB and external hard drives. On this record, it is irrelevant whether copies of those recordings were made, whether an FBI employee was involved in making those copies, or whether the originals were still available. In short, posing a series of rhetorical questions and failing to provide any supporting factual or legal analysis is insufficient to establish materiality.

c. Probable Cause Supports the Warrants

A judicial official may issue a search warrant only if it is supported by probable cause. Fed. R. Crim. P. 41(d)(1). "Probable cause is 'is not a high bar.'" *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018) (quoting *Kaley v. United States* 134 S. Ct. 1090, 1103 (2018)). The

judicial official uses a "totality-of-the-circumstances analysis," and "[t]he task" of the official "is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

The remedy in cases where a private actor acts as an instrument of the government in conducting a search or where a *Franks* violation has occurred is the same: excise the tainted probable cause and determine whether the warrant is still supported by sufficient probable cause. *See United States v. Sellers*, 512 F. App'x 319, 328–29 (4th Cir. 2013) ("In this case, setting aside the allegedly impermissible GPS information contained in the wiretap application, the surviving information contained in the application remained sufficient to support a finding of probable cause and necessity required to issue the wiretap."); *United States v. Moses*, 540 F.3d 263, 271 (4th Cir. 2008) ("Accordingly, evidence obtained during entry of the residence may not be considered to support the search warrant subsequently obtained, and we must determine whether, when that evidence is excluded from the application for the warrant, probable cause to support the warrant still existed."); *United States v. Gillenwaters*, 890 F.2d 679, 681 (4th Cir. 1989) (explaining that in a situation where there is a *Franks* violation "the correct course was to set aside the suspect material and make a probable cause evaluation based on what remained of the affidavit").

In this case, the affidavit in support of the search warrant for Defendant's devices is supported by probable cause even without the information provided by Kimberly or Courtney's alleged role in collecting that information. The affidavit describes Defendant's admissions that he obtained images of teen girls from a website called "teen gallery." Defendant said that he transformed these images into naked images of the minors. He described one such image as an

image of an ex-girlfriend when she was a minor, and he admitted that he masturbated to it. He further admitted to saving these images to a zip or thumb drive, as well as an external hard drive. His admissions, without more, were sufficient probable cause to obtain the warrant and search his devices. Accordingly, the warrant survives and Defendant's motion to suppress should be denied.

d. Good Faith Exception Applies

In *Bonds*, this Court set forth the standard for the application of the Good Faith Doctrine to a deficient warrant.

> Under the good faith exception to the exclusionary rule, evidence obtained by an officer who acts in objectively reasonable reliance on a search warrant will not be suppressed, even if the warrant is later deemed invalid. *United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018) (citing *United States v. Leon*, 468 U.S. 897, 922, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984)).
>
> Evidence obtained from an invalidated warrant "will be suppressed only if 'the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause.'" *United States v. Fall*, 955 F.3d at 371 (citing *United States v. Lalor*, 996 F.2d 1578, 1583 (4th Cir. 1993)).
>
> In determining whether to suppress the fruits of an unconstitutional search, the Court must undertake a "rigorous" cost-benefit analysis, weighing the "deterrence benefits of exclusion" against its "substantial social costs." *Davis v. United States*, 564 U.S. 229, 237–38 (2011). Those costs include interfering with courts' truth-seeking function, and more specifically, concealing "reliable, trustworthy evidence bearing on guilt or innocence" and, in some instances, "set[ting] the criminal loose in the community without punishment." *Davis*, 564 U.S. at 237. Exclusion is a "bitter pill" swallowed only where it would result in a "substantial deterrent effect" that outweighs its resulting costs. *United States v. Leon*, 468 U.S. 897, 907 n.6, (1984).

Bonds, 2021 WL 4782270, at 4-5. "A *Franks* violation is not subject to the good-faith exception to the usual remedy of suppression." *United States v. Hall*, No. 20-4618, 2021 WL 5754904, at *4 n.1 (4th Cir. Dec. 3, 2021); *United States v. Leon,* 468 U.S. 897, 910 (1984) (noting that good faith exception is not applicable where the magistrate was misled by false information knowingly or recklessly submitted by the affiant).

Here, the affiant reasonably relied on the warrant. The affiant received information from Kimberly, who simply acted as a tipster. He corroborated that information by reviewing the recordings Kimberly made on USB B and by interviewing Defendant. There is no conduct in this case that needs to be deterred.

Additionally, the cost of suppression would be high. The affiant did not simply take Kimberly's word for it. She made a recording of what she saw, and the affiant reviewed that recording. Moreover, the evidence in this case has nothing to do with Kimberly's recordings. The evidence comes from the devices that were seized and the forensics associated with those devices. "These files are reliable, trustworthy evidence bearing on guilt or innocence of the Defendant in this case and suppression of them would interfere with the truth-seeking function of this Court." *See Bonds*, 2021 WL 4782270, at 5. Accordingly, suppression is not an appropriate remedy and the motion to suppress and should be denied on the additional ground of the affiant's good faith.

III. Conclusion

For the reasons explained above, the Defendant's Motion to Suppress and Request for Evidentiary Hearing should be denied.

RESPECTFULLY SUBMITTED, April 26, 2023.

DENA J. KING
UNITED STATES ATTORNEY

By: /s/ *Daniel Cervantes*
Daniel Cervantes
Assistant United States Attorney
FL Bar Number: 40836
Attorney for the United States
United States Attorney's Office
227 West Trade Street, Suite 1650
Charlotte, North Carolina 28202
Telephone: 704.338.3115
Fax: 704.227.0197
E-mail: daniel.cervantes@usdoj.gov

By: */s/ Mark T. Odulio*

Mark T. Odulio
Assistant United States Attorney
North Carolina Bar Number: 50011
United States Attorney's Office
227 West Trade Street, Suite 1700
Charlotte, North Carolina 28202
Telephone: 704.338.3108
Fax: 704.344.6629
E-mail: Mark.Odulio@usdoj.gov